

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-160832

(43)Date of publication of application : 20.06.1997

(51)Int.Cl.

G06F 12/14

G06F 3/06

G06F 12/16

(21)Application number : 07-317894

(71)Applicant : HITACHI LTD

(22)Date of filing : 06.12.1995

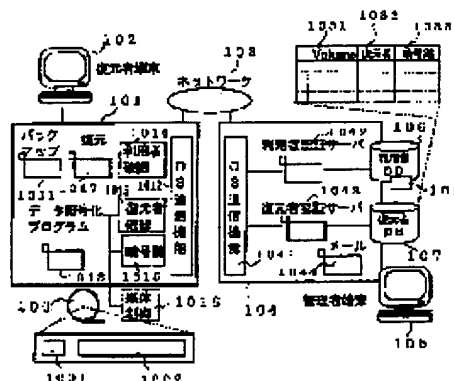
(72)Inventor : DOMYO SEIICHI
KURODA SAWAKI
KAMIYAMA ZENSHI

(54) METHOD AND SYSTEM FOR BACKING UP AND RESTORING DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To keep backup data secret by receiving a deciphering key for restoring data on a portable medium (tape) from a 2nd computer and deciphering the data on the portable medium with the received deciphering key.

SOLUTION: This system is equipped with a 1st computer 101 on which the tape 100 where the backup data are stored can be loaded, a restorer terminal 102 connected to the 1st computer 101, a 2nd computer 104 connected to the 1st computer 101 through a network 103, and an administrator terminal 105 connected to the 2nd computer 104. When the backup data stored on the tape 100 are restored, a user DB 106 and a restorer DB 107 arranged on the side of the 2nd computer 104 are used to authorize the user and restorer on-line and only the user who is registered as a regular user or restorer is allowed to decipher the data on the tape 100.



LEGAL STATUS

[Date of request for examination] 06.09.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3481755

[Date of registration] 10.10.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-160832

(43) 公開日 平成9年(1997)6月20日

(51) Int.Cl. ⁹	識別記号	片内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
3/06	3 0 4		3/06	3 0 4 M
12/16	3 1 0	7623-5B	12/16	3 1 0 M

審査請求 未請求 請求項の数6 O L (全 16 頁)

(21) 出願番号 特願平7-317894

(22) 出願日 平成7年(1995)12月6日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 道明 誠一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 黒田 沢希

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 上山 善嗣

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(74) 代理人 弁理士 秋田 収喜

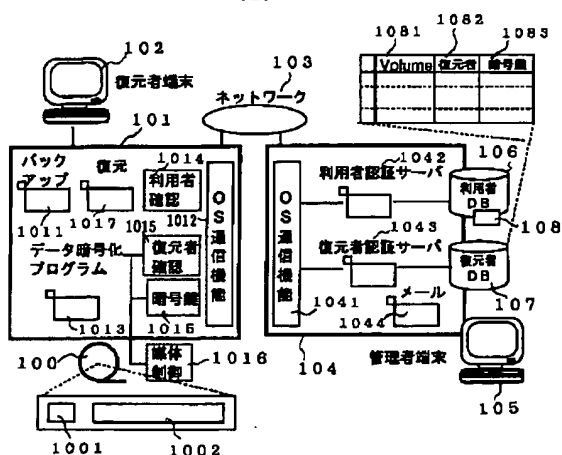
(54) 【発明の名称】 データバックアップ/復元方法およびシステム

(57) 【要約】

【課題】 暗号鍵（復号鍵）の面倒な受渡しを行うことなく、バックアップ作業者が認めた正規の復号者のみに可搬媒体のバックアップデータを復元させ、バックアップデータの秘密性、安全性を保持すること。

【解決手段】 可搬媒体にデータをバックアップする際に、バックアップ作業者が指定した暗号鍵で暗号化して可搬媒体に格納すると共に、バックアップ作業者が「復元処理の実行」を認めた複数の復元者のIDと、バックアップデータを格納した可搬媒体のボリュームIDと、暗号鍵とを復元者DBに登録しておき、バックアップデータを復元する際には、可搬媒体のボリュームIDと1組になっている複数の復元者のIDを読み出し、復元しようとする者が入力したIDに一致する復元者IDが存在する場合のみ、その復元者が入力した復号鍵または第2の計算機から送信されて来た復号鍵によって可搬媒体の暗号化データを復号を許す。

図 1



【特許請求の範囲】

【請求項1】 可搬媒体に対してデータをバックアップすると共に、そのバックアップしたデータを復元する第1の計算機と、この第1の計算機にネットワーク経由で接続された第2の計算機を備えた分散システムにおけるデータバックアップ／復元方法であって、前記第1の計算機で可搬媒体にデータをバックアップする際に、バックアップするデータの復元を許す少なくとも1人の復元者識別情報を入力するステップと、バックアップするデータの暗号鍵を入力するステップと、可搬媒体の識別子を検出するステップと、前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報を第2の計算機に送付し、第2の計算機が管理するデータベースに登録させるステップと、バックアップ対象のデータを前記暗号鍵によって暗号化して前記可搬媒体に格納するステップと、前記可搬媒体から暗号化したバックアップデータを第1の計算機で復元する際に、復元者の識別情報を入力するステップと、復元対象の可搬媒体の識別子を検出するステップと、可搬媒体の識別子と復元者の識別情報とを第2の計算機に送信し、前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かの認証を受けるステップと、正規の復元者である旨の認証結果を受け、可搬媒体のデータを復元するための復号鍵を入力するステップと、入力された復号鍵によって可搬媒体のデータを復号するステップとを備えることを特徴とするデータバックアップ／復元方法。

【請求項2】 可搬媒体に対してデータをバックアップすると共に、そのバックアップしたデータを復元する第1の計算機と、この第1の計算機にネットワーク経由で接続された第2の計算機を備えた分散システムにおけるデータバックアップ／復元方法であって、前記第1の計算機で可搬媒体にデータをバックアップする際に、バックアップするデータの復元を許す少なくとも1人の復元者識別情報を入力するステップと、バックアップするデータの暗号鍵を入力するステップと、可搬媒体の識別子を検出するステップと、前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報を第2の計算機に送付し、第2の計算機が管理するデータベースに登録させるステップと、バックアップ対象のデータを前記暗号鍵によって暗号化して前記可搬媒体に格納するステップと、前記可搬媒体から暗号化したバックアップデータを第1の計算機で復元する際に、

復元者の識別情報を入力するステップと、復元対象の可搬媒体の識別子を検出するステップと、可搬媒体の識別子と復元者の識別情報とを第2の計算機に送信し、前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かの認証を受けるステップと、正規の復元者である旨の認証結果により、可搬媒体のデータを復元するための復号鍵を第2の計算機から受信するステップと、

10 受信された復号鍵によって可搬媒体のデータを復号するステップとを備えることを特徴とするデータバックアップ／復元方法。

【請求項3】 前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報は、データをバックアップする可搬媒体とは異なる可搬媒体に記録して第2の計算機の管理者に送付することを特徴とする請求項1または2記載のデータバックアップ／復元方法。

【請求項4】 前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報は、前記ネットワーク経由で第2の計算機に送信し、第2の計算機の処理によって前記データベースに登録することを特徴とする請求項1または2記載のデータバックアップ／復元方法。

【請求項5】 可搬媒体に対してデータをバックアップすると共に、そのバックアップしたデータを復元する第1の計算機と、この第1の計算機にネットワーク経由で接続された第2の計算機を備えた分散システムにおいて、

前記第1の計算機は、バックアップするデータの復元を許す少なくとも1人の復元者識別情報を入力する手段と、バックアップするデータの暗号鍵を入力する手段と、可搬媒体の識別子を検出する手段と、前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報を第2の計算機に送付し、第2の計算機が管理するデータベースに登録させる手段と、バックアップ対象のデータを前記暗号鍵によって暗号化して前記可搬媒体に格納する手段と、前記可搬媒体から暗号化したバックアップデータを復元する復元者の識別情報を入力する入力手段と、

40 可搬媒体の識別子と復元者の識別情報とを第2の計算機に送信し、前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かの認証を受ける手段と、正規の復元者である旨の認証結果を受け、可搬媒体のデータを復元するための復号鍵を入力する手段と、入力された復号鍵によって可搬媒体のデータを復号する手段とを備え、

前記第2の計算機は、前記第1の計算機から送付された可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報をデー

50

データベースに登録する手段と、

第1の計算機から受信した可搬媒体の識別子と復元者の識別情報と前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かを認証し、その認証結果をネットワーク経由で第1の計算機に返信する手段とを備えることを特徴とする分散システム。

【請求項6】 可搬媒体に対してデータをバックアップすると共に、そのバックアップしたデータを復元する第1の計算機と、この第1の計算機にネットワーク経由で

接続された第2の計算機を備えた分散システムにおいて、

前記第1の計算機は、

可搬媒体にバックアップするデータの復元を許す少なくとも1人の復元者識別情報を入力する手段と、

バックアップするデータの暗号鍵を入力する手段と、

可搬媒体の識別子を検出する手段と、

前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報を第2の計算機に送付し、第2の計算機が管理するデータベースに登録させる手段と、

バックアップ対象のデータを前記暗号鍵によって暗号化して前記可搬媒体に格納する手段と、

前記可搬媒体から暗号化したバックアップデータを復元する復元者の識別情報を入力する手段と、

可搬媒体の識別子と復元者の識別情報とを第2の計算機に送信し、前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かの認証を受ける手段と、

正規の復元者である旨の認証結果により、可搬媒体のデータを復元するための復号鍵を第2の計算機から受信する手段と、

受信された復号鍵によって可搬媒体のデータを復号する手段とを備え、前記第2の計算機は、

前記第1の計算機から送付された可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報をデータベースに登録する手段と、

第1の計算機から受信した可搬媒体の識別子と復元者の識別情報と前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かを認証し、正規の復元者である時のみ復元用の復号鍵をネットワーク経由で第1の計算機に返信する手段とを備えることを特徴とする分散システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データバックアップ／復元方法およびシステムに係り、特に、可搬媒体に記憶させたバックアップデータを不正な利用者には復元できないようにするためのデータバックアップ／復元方法およびシステムに関するものである。

【0002】

【従来の技術】計算機技術におけるデータバックアップ方法は、計算機のデータを定期的に磁気テープや磁気ディスク等の可搬媒体（以下、テープと記す）に格納し、障害発生等の要因で計算機上のデータが利用不可になった際に、テープの内容をもとにデータを復元する業務である。

【0003】しかし、このバックアップ作業の問題点として、OS（オペレーティングシステム）が利用者を認証する計算機上に比べて、不正な利用者がテープのデータをアクセスする可能性が高いことが挙げられる。

【0004】そこで、バックアップの際に、利用者に暗号鍵を入力させ、その暗号鍵によってテープに格納するデータを暗号化した後、その暗号化したデータをテープに格納する方法がある。

【0005】この方法によれば、暗号鍵に対応する復号用の鍵を入力しなければ、テープのデータを復号することができないため、テープに格納したデータの秘密性あるいは安全性を高めることができる。

【0006】なお、復号用の鍵は、暗号鍵と同じものを用いる秘密鍵方式と、別なものを用いる公開暗号鍵方式がある。

【0007】このように、バックアップ対象のデータに暗号化を施す公知技術の文献として、例えば、Simson Garfinkel、Gene Spafford著、山口英訳、「UNIXセキュリティ」、（アスキー：1993）がある。

【0008】近年、計算機の利用形態の変化に伴い、インターネット、WWWという用語で代表されるように、ネットワーク内に配置された多数の計算機を使った分散システムが増加している。このような分散システムにおいても、上記のようにデータ暗号化手段を用いたデータバックアップが必要である。

【0009】分散システムにおいてデータバックアップを実施する場合、次のようなことが問題となる。

【0010】（1）分散システムでは、計算機が数千台の規模になることがあり、このような場合には作業者と復元者は複数名となる。従って、データをバックアップする利用者（以下、作業者と記す）とデータを復元する利用者（以下、復元者と記す）とが同一人物でないことがあるため、このような場合における復号用の鍵の保管、受け渡しが面倒になる。また、作業者の責任で、暗号鍵および復号鍵をオフラインで管理する運用形態では、復号鍵の管理が煩雑になる。さらに、暗号鍵および復号鍵を盗まれた場合は、データの秘密性を保持できなくなる。

【0011】（2）バックアップを行った計算機と別の計算機でテープ上のデータを復元する場合があるため、その際の利用者の認証方法を定める必要がある。

【0012】（3）暗号鍵や利用者情報および業務の機密を含んだバックアップデータを、たとえ暗号化してい

でもネットワーク上で転送することは極力避ける。

【0013】上記(2)の事項に関しては、システム管理者が厳重に管理する計算機上の利用者DBを参照し、他の計算機の利用者を認証するOSやミドルウェアを導入することで、解決できる。例えば、OSF/DCEと呼ばれる技術であり、Ward Rosenberry、David Kenney & Gerry Fisher 著、Understanding DCE、O'Reilly & Associates、Inc(1992)で開示されている。

【0014】また、上記(3)の事項に関しては、ネットワーク上での盗聴・改ざんを避けるために、専門業者によるテープの送付などの運用方法によって解決できる。

【0015】

【発明が解決しようとする課題】しかし、上述した(1)の事項に関しては、これを解決する有効な公知技術は見あたらない。

【0016】本発明の目的は、復号用の鍵の面倒な受渡し作業および保管作業を行うことなく、作業者が認めた正規の復号者のみにバックアップデータの復号を許し、バックアップデータの秘密性を保持することができるデータバックアップ/復元方法およびシステムを提供することにある。

【0017】

【課題を解決するための手段】上記目的達成のため、本発明のデータバックアップ方法は、前記第1の計算機で可搬媒体にデータをバックアップする際に、バックアップするデータの復元を許す少なくとも1人の復元者識別情報を入力するステップと、バックアップするデータの暗号鍵を入力するステップと、可搬媒体の識別子を検出するステップと、前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報を第2の計算機に送付し、第2の計算機が管理するデータベースに登録させるステップと、バックアップ対象のデータを前記暗号鍵によって暗号化して前記可搬媒体に格納するステップと、前記可搬媒体から暗号化したバックアップデータを第1の計算機で復元する際に、復元者の識別情報を入力するステップと、復元対象の可搬媒体の識別子を検出するステップと、可搬媒体の識別子と復元者の識別情報とを第2の計算機に送信し、前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かの認証を受けるステップと、正規の復元者である旨の認証結果を受け、可搬媒体のデータを復元するための復号鍵を入力するステップと、入力された復号鍵によって可搬媒体のデータを復号するステップとを備えることを特徴とする。

【0018】この場合、正規の復元者である旨の認証結果により、可搬媒体のデータを復元するための復号鍵を第2の計算機から受信し、その受信された復号鍵によって可搬媒体のデータを復号するように構成することができる。

【0019】また、可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報は、データをバックアップする可搬媒体とは異なる可搬媒体に記録して第2の計算機の管理者に送付する方法、あるいはネットワーク経由で第2の計算機に送信し、第2の計算機の処理によって前記データベースに登録する方法を用いることができる。

【0020】また、正規の復元者として認証されない場合、可搬媒体の復元を停止すると共に、システムの管理者に可搬媒体の不正使用を通知するように構成することができる。

【0021】また、可搬媒体にデータをバックアップする前に、可搬媒体の識別子を検出し、その識別子とバックアップ作業者の識別子とを第2の計算機に送付し、他者が暗号化した可搬媒体でないことを確認した後に、バックアップを開始するように構成することができる。

【0022】上記本発明のデータバックアップ/復元方法を実現するシステムは、データを復元する第1の計算機と、この第1の計算機にネットワーク経由で接続された第2の計算機を備え、前記第1の計算機は、バックアップするデータの復元を許す少なくとも1人の復元者識別情報を入力する手段と、バックアップするデータの暗号鍵を入力する手段と、可搬媒体の識別子を検出する手段と、前記可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報を第2の計算機に送付し、第2の計算機が管理するデータベースに登録させる手段と、バックアップ対象のデータを前記暗号鍵によって暗号化して前記可搬媒体に格納する手段と、前記可搬媒体から暗号化したバックアップデータを復元する復元者の識別情報を入力する入力手段と、可搬媒体の識別子と復元者の識別情報とを第2の計算機に送信し、前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かの認証を受ける手段と、正規の復元者である旨の認証結果を受け、可搬媒体のデータを復元するための復号鍵を入力する手段と、入力された復号鍵によって可搬媒体のデータを復号する手段とを備え、前記第2の計算機は、前記第1の計算機から送付された可搬媒体の識別子、復元者識別情報および暗号鍵とから成る1組の情報をデータベースに登録する手段と、第1の計算機から受信した可搬媒体の識別子と復元者の識別情報と前記データベース中の情報と照合することにより、復元者がデータベース中に予め登録されている正規の復元者であるか否かを認証し、その認証結果をネットワーク経由で第1の計算機に返信する手段とを備えることを特徴とする。

【0023】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して詳細に説明する。

【0024】図1は、本発明のデータバックアップ方法を実施する分散システムの実施形態を示すシステム構成

図である。

【0025】この実施形態の分散システムは、バックアップデータを格納するテープ100または既に格納したテープを装着可能な第1の計算機101と、この第1の計算機101に接続された復元者端末102と、第1の計算機101とネットワーク103経由で接続された第2の計算機104と、この第2の計算機104に接続された管理者端末105とを備え、テープ100に格納されたバックアップデータを復元する際に、第2の計算機104側に配置された利用者DB106および復元者DB107を利用し、利用者認証と復元者認証とをオンラインで行い、正規の利用者または復元者として登録されている者のみに、テープ100のデータの復号を許可するようにしたものである。

【0026】ここで、バックアップデータを格納したテープ202は、その内部に当該テープをユニークに識別するボリュームID1001とデータ領域1002とを有している。

【0027】また、第1の計算機101は、バックアッププログラム1011と通信機能を持ったOS1012とを有し、さらにデータ暗号化プログラム1013を有している。

【0028】OS1012には、利用者確認プログラム1014、復元者確認プログラム1015、暗号鍵管理プログラム1015、媒体制御機構1016および復元プログラム1017が含まれている。

【0029】利用者あるいは復元者は、復元者端末102で起動コマンドを入力することにより、復元プログラム1017あるいはデータ暗号化プログラム1013を起動し、テープ100に対するデータのバックアップ処理あるいはバックアップデータの復元を行う。

【0030】一方、第2の計算機104は、第1の計算機101のOS1012との間でネットワーク103を介して接続されるOS1041と、利用者認証を行う利用者認証サーバプログラム1042、復元者認証を行う復元者認証サーバプログラム1043とを備えている。

【0031】利用者DB106には、利用者が予め登録された正規の者であるか否かを識別するための利用者ID108を格納している。

【0032】一方、復元者DB270には、テープ100を識別するためのボリュームID1081、当該テープの復元を許可された正規の復元者を示す復元者ID1082、当該テープのバックアップデータを復元するための暗号鍵1083とから成る1組の情報がテープ100のボリュームID別に予め格納されている。

【0033】ここで、復元者DB270における復元者ID1082は、1つのテープ100につき複数人分登録することができる。

【0034】以上のように構成されたシステムにおけるバックアップ処理およびデータ復元処理について図2の

フローチャートを用いて説明する。

【0035】バックアップ処理

まず、利用者が復元者端末102を介してバックアッププログラム1011を起動する。バックアッププログラム1011は、バックアップ処理を開始する前に利用者が正規の者であるか否かを確認するために、利用者確認プログラム220を呼び出す。

【0036】利用者確認プログラム1014は、OS1012の通信機能およびネットワーク103を通じて第2の計算機104の利用者認証サーバ1042を呼び出す。そして、復元者が復元者端末102から入力した利用者IDを送信する。

【0037】利用者認証サーバ1042は、利用者DB106から該DB106に予め登録されている複数の利用者ID108を取得する。そして、その利用者ID108の中に利用者が復元者端末102から今回入力した利用者IDと一致するものがあるか否かを調べ、一致するものがあれば、当該利用者は正規の利用者であると認証する(ステップ200)。

【0038】一致する利用者IDが登録されていなければ、不正使用者であるので、その旨をバックアッププログラム1001に通知すると共に、復元者端末102の画面に不正使用者であることを表示し、バックアッププログラム1001に対して以降の処理を中止させる。

【0039】正規の利用者であることが確認された場合、バックアッププログラム1001は、テープ100を所定の装着口に装着するように復元者端末102を通じて利用者に通知する。

【0040】そこで、認証された利用者がバックアッププログラム1001の操作指示に従い、テープ100を所定の装着口へ装着すると、バックアップ本処理を開始する。

【0041】このバックアップ本処理では、まず、媒体制御機構1016を介してテープ100のボリュームID1001を読み取る(ステップ211)。

【0042】次に、バックアッププログラム1011は利用者の暗号鍵を入力するように復元者端末102の画面で指示する(ステップ212)。

【0043】暗号鍵が入力されたならば、バックアッププログラム1011はその入力された暗号鍵をデータ暗号化プログラム1013に伝達し、該暗号化プログラム1013にバックアップすべきデータを暗号化させ(ステップ212)、テープ100に格納させる(ステップ214)。この場合、暗号化すべきバックアップデータは図示しないメモリに格納されたものである。

【0044】データ暗号化プログラム1013では、バックアップ本処理の終了後、復元者の登録を行う。この際に、バックアップ処理を実施した利用者以外に復元者が存在するか否かの回答を利用者に求める。そこで、例えばバックアップ作業者が部長で、その部下の課長およ

び係長にも復元を認めるような場合は、復元者端末102より利用者自身が認める他の復元者ID（あるいは復元者氏名）を復元者端末102から入力する（ステップ220, 221）。

【0045】バックアッププログラム1011は、以上のステップで得られたテープ1100のボリュームID、復元者ID、暗号鍵の情報を復元者DB107に登録するための処理を行う。

【0046】復元者DB107への登録方法としては、管理者端末105より手入力で行う方法と、情報を簡単に輸送するカード（例えばフロッピディスク＝FD）に情報を格納し、そのカードを第2の計算機の管理者に送付し、管理者の操作によってカード内の情報を復元者DB107へ登録する2つの方法がある。

【0047】そこで、例えばカード（例えばフロッピディスク＝FD）にボリュームID、復元者ID、暗号鍵の情報を格納して復元者DB107へ格納する方法が利用者によって選択された場合、バックアッププログラム1011はカードが復元者端末102の所定の装着口に装着されたことを検出し、そのカードにボリュームID、復元者ID、暗号鍵の情報を格納する（ステップ231, 232）。

【0048】利用者は、そのカードを管理者宛に送付する（ステップ233）。

【0049】カードを受け取った管理者は、そのカードを管理者端末の所定の装着口に装着し（あるいは挿入し）、カード内の情報を読み取らせ、第2の計算機104の復元者認証サーバ1043を通じて復元者DB107へ登録させる（ステップ234, 235）。

【0050】ボリュームID、復元者ID、暗号鍵の情報を手入力で登録する方法が利用者によって選択された場合、ボリュームID、復元者ID、暗号鍵の情報を表示または印刷するなどの方法によって利用者に通知する。利用者は、この通知されたボリュームID、復元者ID、暗号鍵の情報を管理者端末105の設置場所に赴き、管理者端末105から手入力する。あるいは、管理者に連絡して管理者に手入力してもらう（ステップ236）。

【0051】これによって、復元者DB107には、テープ100に今回バックアップしたボリュームID1081、復元者ID1082、暗号鍵1083から成る1組の情報がボリュームID別に格納される。

【0052】バックアップデータの復元処理

次に、テープ100に格納されたバックアップデータの復元処理について説明する。

【0053】まず、復元者が復元者端末102を介して復元プログラム1017を起動する。復元プログラム1017は、復元処理を開始する前に復元者が正規の利用者であるか否かを確認するために、利用者確認プログラム1014を呼び出す。

【0054】利用者確認プログラム1014は、OS1012の通信機能およびネットワーク103を通じて第2の計算機104の利用者認証サーバ1042を呼び出す。そして、復元者が復元者端末102から入力した復元者IDを送信する。

【0055】復元者IDを受信した利用者認証サーバ1042は、利用者DB106から該DB106に予め登録されている複数の利用者ID108を取得する。そして、その利用者ID108の中に第1の計算機101から受信した復元者IDと一致するものがあるか否かを調べ、一致するものがあれば、当該復元者は正規の利用者であると認証する（ステップ250）。

【0056】一致する利用者IDが登録されていなければ、不正使用者であるので、その旨をOS10412の通信機能およびネットワーク103を通じて第1の計算機101の利用者確認プログラム1014、復元プログラム1017に通知し、復元者端末102の画面に不正使用者であることを表示し、復元プログラム1017に対して以降の復元処理を中止させる（ステップ271）。

さらに、管理者端末105に対し、不正使用者で旨のメール1044を送信し、管理者端末105の画面に不正使用者で旨のメッセージを表示させ、管理者に通知する（ステップ272）。

【0057】正規の利用者であることが確認された場合（ステップ260）、復元プログラム1017は、テープ100を所定の装着口に装着するように復元者端末102を通じて復元者に通知する。

【0058】そこで、認証された復元者が復元プログラム1017の操作指示に従い、テープ100を所定の装着口へ装着すると、復元本処理（ステップ280）を開始する。

【0059】この復元本処理では、まず、媒体制御機構1016を介してテープ100のボリュームID1001を読み取る（ステップ281）。

【0060】次に、復元プログラム1017は復元者確認プログラム1015を呼び出す。

【0061】復元者確認プログラム1017は、テープ100のボリュームID1001に対応した復元者IDを取得するために、OS1012の通信機能およびネットワーク103を通じて第2の計算機104の復元者認証サーバ1043を呼び出し、ステップ281で取得したテープ100のボリュームID1001と、ステップ250で認証して復元者の利用者IDを送信する。

【0062】復元者認証サーバ1043は、この復元者認証サーバ1043を通じて、復元者DB107からボリュームID1001に対応する複数の復元者ID1082を取得する。すなわち、バックアップ作業者が予め認めている複数の復元者ID1082を取得する。

【0063】そして、その復元者ID1082の中に、ステップ250で認証した利用者IDと一致するものが

あるか否かを調べ、一致するものがあれば、当該復元者はバックアップ作業者が予め認めている正規の復元者であると認証する(ステップ282、283)。この場合、ステップ250で認証した利用者IDは、利用者認証サーバ1042から取得するようにしてもよい。

【0064】一致する復元者ID1082が登録されていなければ、不正復元者であるので、その旨をデータ暗号化プログラム1013および復元プログラム1017に通知し、復元プログラム1017によって復元者端末102の画面に不正使用者であることを表示させ、さらにデータ暗号化プログラム1013に対して以降の復元処理を中止させる(ステップ291)。また、管理者端末105に対しても不正使用者で旨のメール1044を送信し、管理者端末105の画面に不正使用者で旨のメッセージ表示させ、管理者に通知する(ステップ292)。

【0065】正規の復元者であることが確認された場合(ステップ283)、復号プログラム1017は復号鍵(暗号鍵と同じ鍵)を入力するように復元者端末102の画面で指示する(ステップ284)。

【0066】復号鍵が入力されたならば、その復号鍵をデータ暗号化プログラム1013に伝達する。データ暗号化プログラム1013は、媒体制御機構1016を通じてテープ100に格納されたデータを読み出し、その読み出しデータを復号鍵で復号し(ステップ285)、復元プログラム1017に渡す。

【0067】これにより、テープ100のデータ領域1002に暗号化されて格納されたデータが復元される(ステップ286)。

【0068】図3は、図2におけるステップ250、260、270の処理の際のプログラムの関係を示したものである。特に、ステップ270の停止処理内部では、利用者認証サーバ1042が復元処理の停止指示を復元プログラム1017に伝達し、さらに管理者端末105へメール1044によって不正使用者で旨のメールを伝達していることを示している。

【0069】図4は、図2におけるステップ282、283、290の処理の際のプログラムの関係を示したものである。特に、ステップ290の停止処理の内部では、復元者認証サーバ1043が復元処理の停止指示をデータ暗号化プログラム1013に伝達し、さらに管理者端末105へメール1044によって不正使用者で旨のメールを伝達していることを示している。

【0070】以上のように、本実施形態においては、データをテープ100にバックアップする際に、バックアップ対象のデータをバックアップ作業者が指定した暗号鍵で暗号化してテープ100に格納すると共に、バックアップ作業者が「復元処理の実行」を認めた複数の復元者のIDと、バックアップデータを格納したテープ100のボリュームIDと、暗号鍵とをシステム管理者が管

理している復元者DBに登録しておき、テープ100のデータを復元する際には、テープ100のボリュームIDと1組になっている複数の復元者のIDを読み出し、復元しようとする者が入力したIDに一致する復元者IDが存在するか否かを調べ、一致する復元者IDが存在する場合は、復元しようとする者はバックアップ作業者に「復元処理の実行」を認められた正規の復元者であると認証し、その復元者が入力した復号鍵によってテープ100の暗号化データを復号を許すようにしている。

10 【0071】従って、バックアップ作業者は「復元処理の実行」を認める者に対して暗号鍵(復号鍵)を予め教えておいた上で、その「復元処理の実行」を認める者のIDを復元者DB107に登録しておけば、暗号鍵(復号鍵)の面倒な受渡しを行うことなく、バックアップ作業自身が認めた正規の復号者のみにテープ100のバックアップデータを復元させることができ、バックアップ作業者が認めていない部外者にバックアップデータの秘密性を保持することが可能になる。

20 【0072】なお、復元処理を行う際に、復元しようとする者に復号鍵を入力させているが、復元者DB107には復元者IDと共に暗号鍵1083が登録されているので、この暗号鍵1083によって暗号化データを暗号するようにしてもよい。この場合には、バックアップ作業者は「復元処理の実行」を認める者に対して暗号鍵(復号鍵)を予め教えておく必要はなくなる。

【0073】本発明の第2の実施形態

上述の実施形態では、暗号鍵をバックアップ作業者が入力し、カード(例えばフロッピディスク)に格納して分散システムの管理者が管理している復元者DB(データベース)に登録しておくものであるが、送信データの暗号化して送るメールやRPC(リモートプロセッサコール)を使うことにより、ネットワーク103を介して暗号鍵や復元者IDを登録することもできる。

【0074】図5は、暗号鍵や復元者IDをネットワーク103経由で第2の計算機104の復元者DB107に登録する手順を示すフローチャートである。

【0075】まず、利用者(バックアップ作業)が復元者端末102を介してバックアッププログラム1011を起動する。バックアッププログラム1011は、バックアップ処理を開始する前に利用者が正規の利用者であるか否かを確認するために、利用者確認プログラム1014を呼び出す。

【0076】利用者確認プログラム1014は、OS1012の通信機能およびネットワーク103を通じて第2の計算機104の利用者認証サーバ1042を呼び出す。そして、利用者が復元者端末102から入力した利用者IDを送信する。

【0077】利用者IDを受信した利用者認証サーバ1042は、利用者DB106から該DB106に予め登

録されている複数の利用者ID108を取得する。そして、その利用者ID108の中に第1の計算機101から受信した利用者IDと一致するものがあるか否かを調べ、一致するものがあれば、当該利用者は正規の利用者であると認証する(ステップ501)。

【0078】一致する利用者IDが登録されていなければ、不正使用者であるので、その旨をOS1042の通信機能およびネットワーク103を通じて第1の計算機101の利用者確認プログラム1014、バックアッププログラム1011に通知し、復元者端末102の画面に不正使用者であることを表示し、バックアッププログラム1011に対して以降のバックアップ処理を中止させる。さらに、管理者端末105に対し、不正使用者で旨のメール1044を送信し、管理者端末105の画面に不正使用者で旨のメッセージを表示させ、管理者に通知する。

【0079】正規の利用者であることが確認された場合(ステップ260)、バックアッププログラム1011は、テープ100を所定の装着口に装着するように復元者端末102を通じて利用者に通知する。

【0080】そこで、認証された利用者がバックアッププログラム1011の操作指示に従い、テープ100を所定の装着口へ装着すると、バックアップ本処理(ステップ510)を開始する。

【0081】このバックアップ本処理では、まず、媒体制御機構1016を介してテープ100のボリュームID1001を読み取る(ステップ511)。

【0082】次に、バックアッププログラム1011は利用者の暗号鍵を入力するように復元者端末102の画面で指示する(ステップ512)。

【0083】暗号鍵が入力されたならば、さらに、バックアップ処理を実施した利用者以外の複数の復元者IDを入力するように復元者端末102の画面で指示する(ステップ513)。

【0084】バックアッププログラム1011はその入力された暗号鍵をデータ暗号化プログラム1013に伝達し、該暗号化プログラム1013にバックアップすべきデータを暗号化させ(ステップ514)、テープ100に格納させる(ステップ515)。この場合、暗号化すべきバックアップデータは図示しないメモリに格納されたものである。

【0085】次に、データ暗号化プログラム1013は、バックアップ本処理の終了後、復元者登録処理を行う。

【0086】以降は、データ暗号化プログラム1013の処理と復元者認証サーバ1043の応答で手順が進行する。

【0087】復元者登録処理(ステップ520)では、データ暗号化プログラム1013は、利用者ID、ボリュームIDおよび復号者IDを復元者端末102から入

力させる。

【0088】そして、利用者IDを引数にし、OS1012、OS1041を介して復元者認証サーバ1043に接続要求を送信する(ステップ521)。この際、復元者認証サーバ1043は復元者DB107が利用可能ならば接続を許可する(ステップ551)。

【0089】なお、復元者認証サーバ1043が起動されていない場合、再試行で接続できるまで待つか、タイムアウトでバックアップ処理全体を終了する。また、復元者認証サーバ261が必要に応じて送信者の利用者IDをもとに、利用者認証サーバ260に問い合わせる処理を行い(ステップ552)、再認証する。

【0090】次に、ボリュームIDと利用者IDを引数とし、復号鍵および復元者の情報を送信する(ステップ522)。

【0091】復元者認証サーバ1043は、復号鍵および復元者の情報を受信したならば(ステップ553)、復元者DB107を参照し、問い合わせのボリュームID、利用者IDに対応する復号鍵および復元者IDを復元者DB107に登録する(ステップ554)。

【0092】データ暗号化プログラム1013は、復号鍵および復元者IDが登録されたことを確認し、復元者認証サーバ1043とのセッションを切断した後(ステップ523)、送信データを破棄する(ステップ524)。

【0093】本実施形態によれば、ボリュームIDに対応する復号鍵および復元者IDをオンラインで復元者DB107に登録するようにしているため、カード記録媒体に格納して登録する方法に比べて、登録作業が楽になるうえ、カード記録媒体を紛失した場合にバックアップ作業者が認めた他の復元者が復元不可能に陥ってしまうことを防止することができる。

【0094】なお、ステップ522、553において、データの暗号化手順と別なデータ暗号化手順を用いて送信データを暗号化すれば、暗号鍵の盗用を防止することができる。

【0095】図6は、可搬媒体であるテープ100の暗号鍵をオンラインで授受して復元者を認証する手順を示すフローチャートである。

【0096】まず、復元者が復元者端末102を介して復元プログラム1017を起動する。復元プログラム1017は、復元処理を開始する前に利用者が正規の復元者であるか否かを確認するために、利用者確認プログラム1014を呼び出す。

【0097】利用者確認プログラム1014は、OS1012の通信機能およびネットワーク103を通じて第2の計算機104の利用者認証サーバ1042を呼び出す。そして、利用者が復元者端末102から入力した利用者IDを送信する。

【0098】利用者IDを受信した利用者認証サーバ1

042は、利用者DB106から該DB106に予め登録されている複数の利用者ID108を取得する。そして、その利用者ID108の中に第1の計算機101から受信した利用者IDと一致するものがあるか否かを調べ、一致するものがあれば、当該利用者は正規の利用者であると認証する(ステップ601)。

【0099】一致する利用者IDが登録されていなければ、不正使用者であるので、その旨をOS1042の通信機能およびネットワーク103を通じて第1の計算機101の利用者確認プログラム1014、復元プログラム1017に通知し、復元者端末102の画面に不正使用者であることを表示し、復元プログラム1017に対して以降の復元処理を中止させる。さらに、管理者端末105に対し、不正使用者で旨のメール1044を送信し、管理者端末105の画面に不正使用者で旨のメッセージを表示させ、管理者に通知する。

【0100】正規の利用者であることが確認された場合、復元プログラム1017は、テープ100を所定の装着口に装着するように復元者端末102を通じて利用者に通知する。

【0101】そこで、認証された利用者が復元プログラム1017の操作指示に従い、テープ100を所定の装着口へ装着すると、復元プログラム1017は媒体制御機構1016を通じてテープ100のボリュームID1001を検出する(ステップ602)。

【0102】以降、復元プログラム1017の処理と復元者認証サーバ1043の応答で手順が進行する。

【0103】復元プログラム1017は、ステップ601で認証した利用者IDおよびステップ602で検出したボリュームID1001を基に、復号鍵入手処理を実行する(ステップ610)。

【0104】この復号鍵入手処理では、まず、利用者IDを引数にし、OS1012、OS1041を介して復元者認証サーバ1043に接続要求を送信する(ステップ611)。この際、復元者認証サーバ1043は、復元者DB107が利用可能ならば接続を許可する(ステップ651)。復元者認証サーバ1043が起動されていない場合、再試行で接続できるまで待つか、タイムアウトでバックアップ処理全体を終了する。また、復元者認証サーバ1043は、必要に応じて、送信者の利用者IDをもとに利用者認証サーバ260に問い合わせ(ステップ652)、再認証する。

【0105】次に、ボリュームID1001と利用者IDとを引数とし、復号鍵を問い合わせる(ステップ612)。

【0106】復元者認証サーバ1043は、復元者DB107を参照し、問い合わせのボリュームID、利用者IDに対応する復号鍵を検索する(ステップ653)。

【0107】復元者認証サーバ1043は、検索結果の復号鍵を送信する(ステップ654)。この場合、該当

する復号鍵が登録されていなければ、その旨の情報を送信する。

【0108】復元プログラム1017は、復号鍵を受け取ったことを確認した後(ステップ613)、復元者認証サーバとのセッションを切断する(ステップ614)。

【0109】復元者認証サーバ1043は、復号鍵の情報を送信した後に、復元者DB107から該当する媒体に関するレコードを削除する等の方法で、以後同一媒体の復号鍵を入手できないようにする(ステップ655)。

【0110】復号鍵を入手できないときには、既に復号化された、あるいは改ざんされた恐れがある媒体と判断し(ステップ615)、その旨を復元者端末102の画面に出力する等の方法で、作業者に警告し(ステップ630)、復元処理を終了する。

【0111】復号鍵を入手できた場合は、復元本処理(ステップ620)に進む。

【0112】復元本処理では、復号鍵を引数として、データ暗号化プログラム212を起動し、テープ100のデータを読み取り、復号化し(ステップ621)、計算機への復元を行う(ステップ622)。

【0113】この復元処理手順では、ステップ655を設けることにより、複数人の作業者のうち、誰かが復元すれば2度と同じ暗号鍵を利用できないようにすることができる。

【0114】上述の実施例では、復元者の登録と認証の方法について述べたが、本発明は、これに限定されるものではなく、たとえば、他者が暗号化した媒体に上書きを防止する手順に適用できるのはいうでもない。

【0115】本発明の第3の実施形態

図7は、バックアップ処理を行う際に、他者が暗号化した可搬媒体であることをオンラインで自動確認する手順を示すフローチャートである。

【0116】まず、利用者(バックアップ作業員)が復元者端末102を介してバックアッププログラム1011を起動する。バックアッププログラム1011は、バックアップ処理を開始する前に利用者が正規の利用者であるか否かを確認するために、利用者確認プログラム1014を呼び出す。

【0117】利用者確認プログラム1014は、OS1012の通信機能およびネットワーク103を通じて第2の計算機104の利用者認証サーバ1042を呼び出す。そして、利用者が復元者端末102から入力した利用者IDを送信する。

【0118】利用者IDを受信した利用者認証サーバ1042は、利用者DB106から該DB106に予め登録されている複数の利用者ID108を取得する。そして、その利用者ID108の中に第1の計算機101から受信した利用者IDと一致するものがあるか否かを調

べ、一致するものがあれば、当該利用者は正規の利用者であると認証する（ステップ701）。

【0119】一致する利用者IDが登録されていなければ、不正使用者であるので、その旨をOS1042の通信機能およびネットワーク103を通じて第1の計算機101の利用者確認プログラム1014、バックアッププログラム1011に通知し、復元者端末102の画面に不正使用者であることを表示し、バックアッププログラム1011に対して以降のバックアップ処理を中止させる。さらに、管理者端末105に対し、不正使用者で旨のメール1044を送信し、管理者端末105の画面に不正使用者で旨のメッセージを表示させ、管理者に通知する。

【0120】正規の利用者であることが確認された場合、バックアッププログラム1011は、テープ100を所定の装着口に装着するように復元者端末102を通じて利用者に通知する。

【0121】そこで、認証された利用者がバックアッププログラム1011の操作指示に従い、テープ100を所定の装着口へ装着すると、媒体制御機構1016を介してテープ100のボリュームID1001を読み取る。

【0122】以降、バックアッププログラム1011の処理と復元者認証サーバ1043の応答で手順が進行する。

【0123】次に、バックアッププログラム1011は、ステップ701で認証した利用者IDおよびステップ702で検出したボリュームID1001を基に、媒体確認処理を実行する（ステップ710）。

【0124】この媒体確認処理では、まず、利用者IDを引数にし、OS1012、OS1041を介して復元者認証サーバ1043に接続要求を送信する（ステップ711）。この際、復元者認証サーバ1043は復元者DB107が利用可能ならば接続を許可する（ステップ751）。しかし、復元者認証サーバ1043が起動されていない場合は、再試行で接続できるまで待つか、タイムアウトでバックアップ処理全体を終了する。また、復元者認証サーバ1043は、必要に応じて、送信者の利用者IDを基に、利用者認証サーバ260に問い合わせ（ステップ752）、再認証する。

【0125】次に、ボリュームIDを引数とし、当該ボリュームIDに対応する利用者IDを問い合わせる（ステップ712）。

【0126】復元者認証サーバ1043は、復元者DB107を参照し、問い合わせのボリュームIDに対応する利用者IDを検索する（ステップ753）。

【0127】復元者認証サーバ1043は、検索結果の利用者IDをバックアッププログラム1011に送信する（ステップ754）。

【0128】問い合わせのボリュームIDに対応する利

用者IDが登録されていなければ、疎の旨を送信する（ステップ754）。

【0129】バックアッププログラム1011は、問い合わせ結果を受け取ったことを確認し（ステップ713）、復元者認証サーバ1043とのセッションを切断する（ステップ714）。

【0130】次に、バックアッププログラム1011は、受信した利用者IDと先に認証した利用者IDとを比較し、一致しない場合は、テープ100は他者が暗号化した媒体であると判断し（ステップ715）、その旨を復元者端末102の画面に出力する等の方法で、作業者に警告し（ステップ730）、バックアップ処理を終了する。

【0131】復元者DB107に未登録、あるいは受信した利用者IDと先に認証した利用者IDとが一致した場合は、他者が暗号化していない媒体であると判定し、バックアップの本処理（ステップ720）に進む。

【0132】この例の手順によれば、テープ100が利用者以外の者によって暗号化されたものであることをオンラインで確認することができる。そして、バックアップ以前に確認することで、他者が暗号化したテープへの上書きや改ざんを防止することができる。また、利用者IDのみを送受信しているので、従来の利用者認証と同一のプロトコルで実現できる利点がある。

【0133】なお、上記各実施例において用いる暗号化の方法は、秘密鍵方式、公開暗号鍵方式のいずれでもよい。特に、秘密鍵方式の場合、鍵の受け渡し方法が簡便になるので、より効果的である。

【0134】

【発明の効果】以上説明したように、本発明によれば、データをテープ等の可搬媒体にバックアップする際に、バックアップ対象のデータをバックアップ作業者が指定した暗号鍵で暗号化して可搬媒体に格納すると共に、バックアップ作業者が「復元処理の実行」を認めた複数の復元者のIDと、バックアップデータを格納した可搬媒体のボリュームIDと、暗号鍵とを復元者DBに登録しておき、バックアップデータを復元する際には、可搬媒体のボリュームIDと1組になっている複数の復元者のIDを讀出し、復元しようとする者が入力したIDに一致する復元者IDが存在するか否かを調べ、一致する復元者IDが存在する場合は、復元しようとする者はバックアップ作業者に「復元処理の実行」を認められた正規の復元者であると認証し、その復元者が入力した復号鍵または第2の計算機から送信されて来た復号鍵によって可搬媒体の暗号化データを復号を許すようにしている。

【0135】このため、バックアップ作業者は「復元処理の実行」を認める者のIDを復元者DBに登録しておけば、暗号鍵（復号鍵）の面倒な受渡しを行うことなく、バックアップ作業者自身が認めた正規の復号者のみに可搬媒体のバックアップデータを復元させることがで

き、バックアップ作業者が認めていない部外者にバックアップデータが漏れてしまったり、改ざんされてしまうことを防止し、バックアップデータの秘密性、安全性を保持することが可能になる。

【0136】また、可搬媒体のボリュームID、復元者ID、暗号鍵を復元者DBで一括登録し、かつ一元管理しているため、システム管理者の手間を省くことができる。

【0137】また、可搬媒体のデータを復号化する際に、可搬媒体の識別子と利用者の識別子とを復元者DBに問い合わせ、正規の復元者として認証された場合に1度だけ復号鍵を送付するようにしているため、復元者がバックアップ作業から暗号鍵を授受する手間を省くことができる。

【図面の簡単な説明】

【図1】本発明のデータバックアップ方法を実施する分散システムの実施形態を示すシステム構成図である。

【図2】バックアップ処理と復元処理の手順を示すフローチャートである。

【図3】図1の復元処理における利用者認証手順を説明

するための図である。

【図4】図1の復元処理における復元者認証手順を説明するための図である。

【図5】復元者情報をオンラインで自動登録する手順を示すフローチャートである。

【図6】可搬媒体の暗号鍵をオンライン上で授受し、復元者を認証する手順を示す図である。

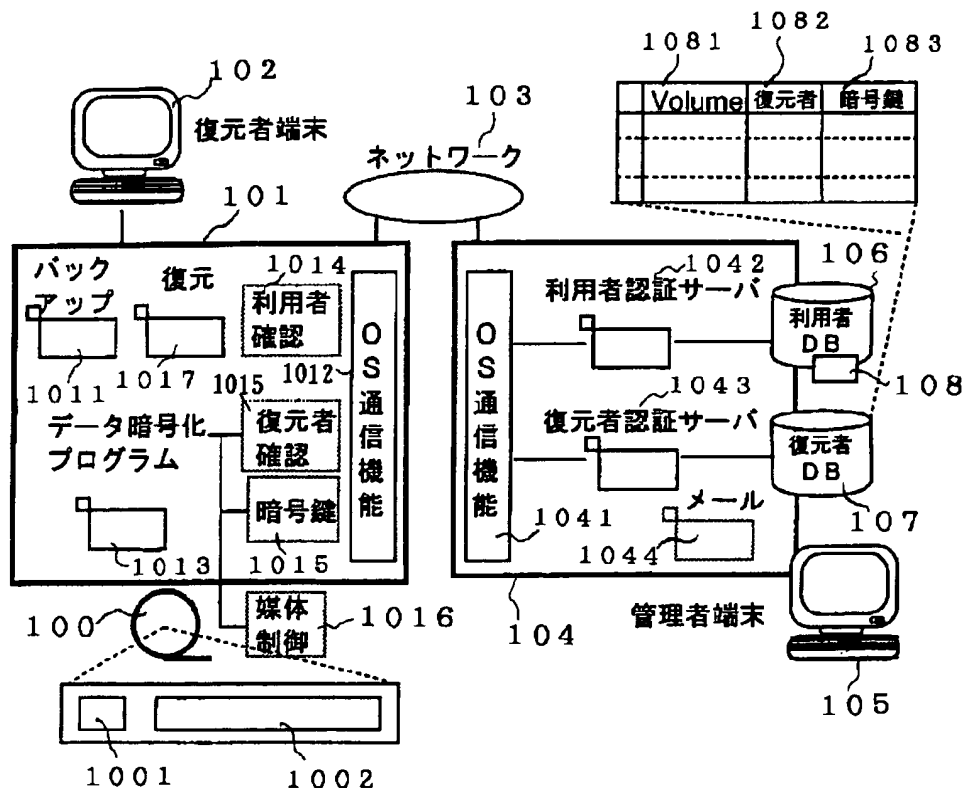
【図7】他者が暗号化した可搬媒体をオンラインで自動確認する手順を示すフローチャートである。

【符号の説明】

100…テープ、101…第1の計算機、102…復元者端末、103…ネットワーク、104…第2の計算機、105…管理者端末、106…利用者DB、107…復元者DB、108…利用者ID、1001…ボリュームID、1011…バックアッププログラム、1013…データ暗号化プログラム、1014…利用者確認プログラム、1015…復元者確認プログラム、1017…復元プログラム、1042…利用者認証サーバ、1043…復元者認証サーバ、1044…メール、1081…暗号鍵、1082…復元者ID、1083…暗号鍵。

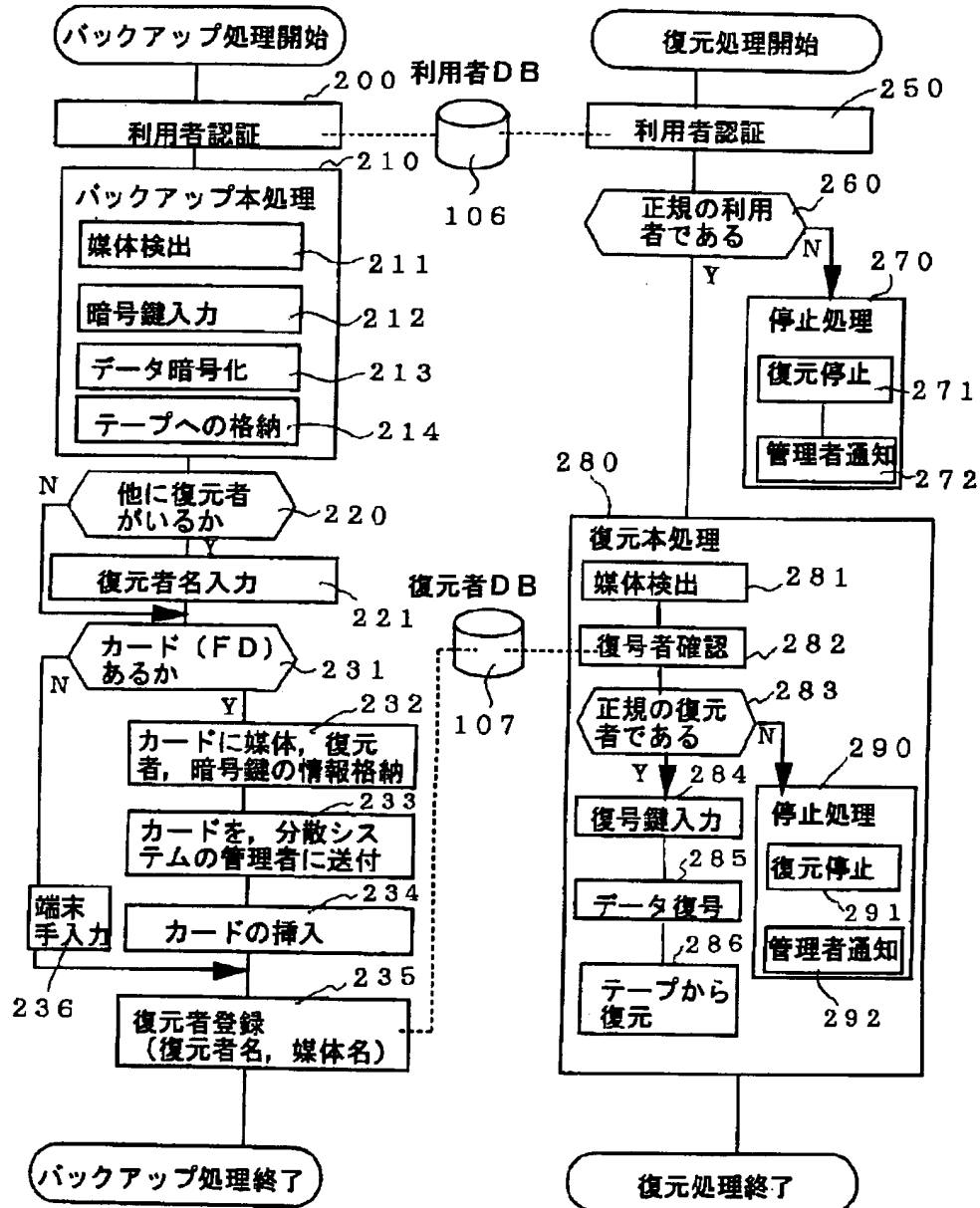
【図1】

図1



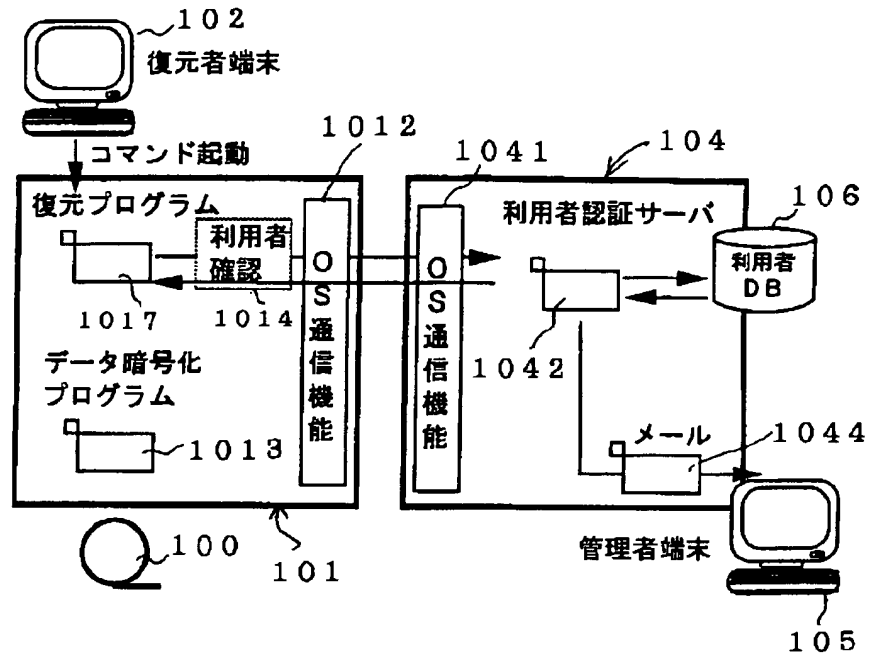
【図2】

図2



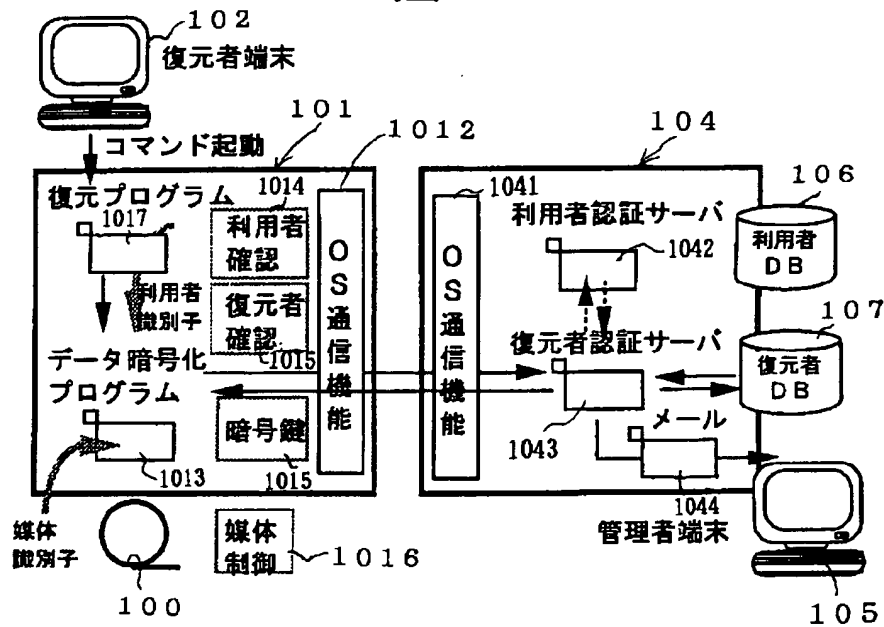
【図3】

図 3



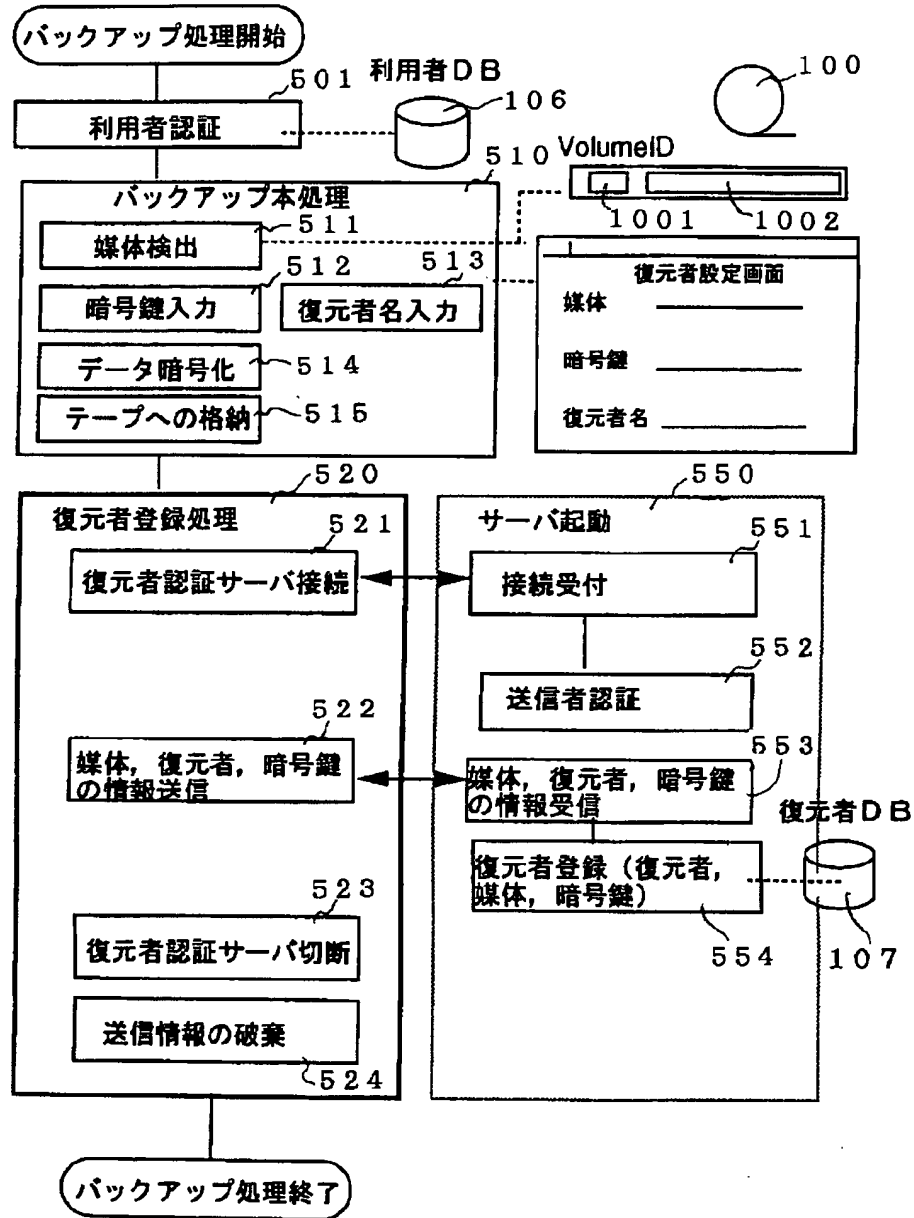
【図4】

図 4



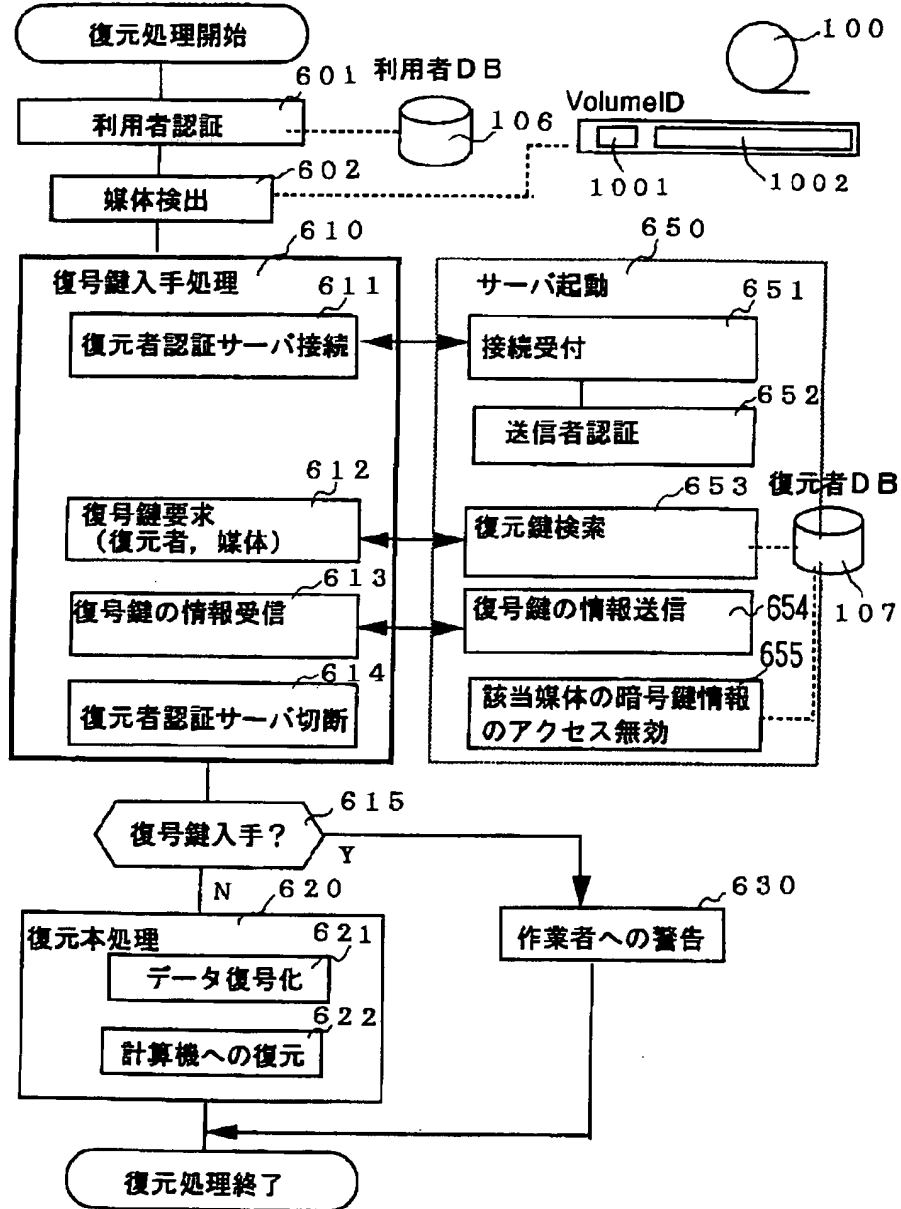
【図5】

図5



【図6】

図 6



【図7】

図7

